UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,927	04/12/2004	Eliot Lear	50325-0864	4441

29989 7590 10/15/2007

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
10/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/822,927	LEAR, ELIOT	
	Examiner	Art Unit	
	Carlton V. Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-21,23-25,27-29 and 31-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-21,23-25,27-29 and 31-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed on **7-20-2007**.

2. Claims **1, 3 - 21, 23 - 25, 27 - 29, 31 - 47** are pending. Claims **1, 21, 25, 29** have been amended. Claims **2, 22, 26, 30** have been cancelled. Claims **33 - 47** are new. Claims **1, 8, 18, 21, 25, 29** are independent.

Response to Arguments

3. Applicant's arguments filed 7/20/2007 have been fully considered but they are not persuasive.

3.1 The amendment filed 7-20-2007 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material, which is not supported by the original disclosure, is as follows:

There is no disclosure within the specification or original claims that two or more principals have collective authority as per amendment to claims. (see Remarks Page 14 and amended claims 1, 21, 25, 29) In addition, the term, *"home network"*, does not exist within the specification and original claims therefore there is no context for usage of this term.

Applicant is required to cancel the new matter in the reply to this Office Action.

3.2 Applicant argues that the referenced prior art does not disclose, *" time period for certificates ". (see Remarks Pages 16-17)*

A certificate for a public/private key pair contains the cryptographic information for the usage of the key pair including an expiration time period. The Bosler prior art indicates a reference that discloses the exchange of certificates and other cryptographic authentication information based on RFC 2246. (see Bosler paragraph [0056], lines 6-10) This reference discloses that the certificate for a public/private key pair can have an expiration time period. (http://www.ietf.org/rfc/rfc2246.txt?number=2246: information for RCF 2246-Transport Layer Security (TLS): see Page 69: check certificate parameter, determine whether certificate has expired based on time period) After the expiration time period, the certificate is no longer considered valid and is considered revoked. Completion of the authentication procedure for a digital signature attached to a management message would indicate whether the certificate has expired or not. The processing of the digital signature would proceed based on the results of the expiration time period check. If the time period has expired, the certificate and digital signature are no longer valid. If the time period has not expired, the certificate and digital signature are valid and can be used for authentication.

3.3 Applicant argues that the referenced prior art does not disclose, " *dependent and new claims and additional features* ". *(see Remarks Page 17-10)*

Due to the successful rejections of the independent claims, the dependent claims (including new claims) have also been successfully rejected. The referenced prior art discloses the limitations of all claims.

3.4 The examiner has considered the applicant's remarks concerning a method and

apparatus for verifying configuration changes for network devices utilizing digital signatures. In one approach, a method comprises receiving configuration information comprising a hostname, one or more configuration directives, and one or more digital signatures subject to verification. The configuration directives are only applied when the one or more digital signatures are successfully verified. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Bosler (20050010757) discloses the applicant's invention including disclosures in Remarks dated July 20, 2007.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims **1, 3 - 21, 23 - 25, 27 - 29, 31 - 47** are rejected under 35 U.S.C. 102(e) as being anticipated by **Bosler et al.** (US Patent No. **20050010757**).

Regarding Claims 1, 21, 25, Bosler discloses a method, comprising the computer

implemented steps of:

a) receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates, received by user)

b) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

c) attempting to verify the one or more digital signatures based on the trust information; (see Bosler paragraph [0008], lines 7-13: verification digital signature based on certificates received from CA (i.e. trust information))

d) verifying that two or more digital signatures, from the one or more digital signatures, are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element; (see Bosler paragraph [0008], lines 7-13; paragraph [0078], lines 7-15: verify digital signature)

e) applying the configuration directives to the host network element only when the one of more digital signatures are verified successfully. (see Bosler paragraph [0057], lines 29-33: utilize directives or commands after digital signature

verification)

Regarding Claims 3, 4, Bosler discloses a method as recited in Claim 1, further comprising the steps of

a) receiving in association with a particular configuration directive, security information defining a number of required signatures and required principals; (see Bosler paragraph [0058], lines 21-28: receive security information with directive (i.e. command, management message))

b) applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-14: digital signature authentication; paragraph [0069], lines 1-5: apply directives or commands after authentication)

Regarding Claims 5, 15, Bosler discloses a, and wherein public keys for the digital signatures are stored on the host. (see Bosler paragraph [0073], lines 4-7: security information stored in central location (i.e. host system), (i.e. option, each individual system or host))

Regarding Claims 6, 16, Bosler discloses a method as recited in Claim 1, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of

attempting to validate the digital signatures. (see Bosler paragraph [0007], lines 6-8: public key cryptography authentication; paragraph [0073], lines 4-7; paragraph [0060], lines 1-6: security information stored in central location or in each individual system or host, certification server (i.e. key server))

Regarding Claims 7, 17, Bosler discloses a method as recited in Claim 1, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13: verification (i.e. validation) with digital signature)

Regarding Claims 8, 18, Bosler discloses a method, comprising the computer implemented steps of:

a) receiving a public key for a user of the network devices; receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates)

b) receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives; (see Bosler paragraph [0071], lines 1-13; paragraph

[0073], lines 77-22: time-based certificate, directive authentication)

c) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date time value; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

d) determining if the date time value is within the time period; (see Bosler paragraph [0073], lines 17-22: time based verification for certificate, time period valid)

e) determining if the one or more configuration directives have been previously received during the time period; (see Bosler paragraph [0069], lines 1-5: process configuration directive(s), commands) and

f) only when the date time value is within the time period (see Bosler paragraph [0073], lines 17-22: time based certificate) and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, and applying the configuration directives to a network element only when the one or more digital signatures are verified successfully. (see Bosler paragraph [0058], lines 5-14: apply directives when digital signature authenticated)

Regarding Claims 9, 10, Bosler discloses a method as recited in Claim 8, wherein the step of determining if the one or more configuration directives have been previously

received during the time period comprises the steps of

a) generating a secure hash of the one or more configuration directives; (see Bosler paragraph [0078], lines 3-15: generate secure hash value for authentication)

b) determining if the secure hash is found in non volatile memory. (see Bosler paragraph [0078], lines 3-15; paragraph [0067], lines 4-8: memory, workspace for data processing: memory (i.e. non-volatile))

Regarding Claim 11, Bosler discloses a method as recited in Claim 8, further comprising the step of storing the secure hash in non volatile memory, in association with an expiration value, when the date time value is within the time period and the one or more configuration directives have not been previously received during the time period. (see Bosler paragraph [0067], lines 4-8: memory, workspace for data processing; paragraph [0071], lines 1-13; paragraph [0073], lines 4-7: time-based certificates; paragraph [0078], lines 3-15: hash (i.e. digest) values utilized for authentication)

Regarding Claim 12, Bosler discloses a method as recited in Claim 8, further comprising the steps of verifying that the one or more digital signatures is valid and that one or more principals respectively associated with the digital signatures have collective authority to perform the directives on the host. (see Bosler paragraph [0058], lines 5-14: mutual authentication required before directive(s) or command(s) implemented)

Regarding Claims 13, 14, Bosler discloses a method as recited in Claim 8, further comprising the steps of

a) receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; (see Bosler paragraph [0058], lines 21-28: key, security information received with directive or command)

b) applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-14; paragraph [0069], lines 1-5: validate digital signature, process directive or command)

Regarding Claim 18, Bosler discloses a method for verifying configuration changes for network devices using digital signatures, comprising the computer implemented steps of:

a) receiving a public key for a user of the network devices; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates (i.e. public key certificate), received by user)

b) receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives to a specified network device; (see Bosler paragraph

[0071], lines 1-13; paragraph [0073], lines 17-22: time based certificate)

c) receiving configuration information comprising a hostname, one or more configuration directives for the specified network device associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date time value; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

d) determining if the date time value is within the time period; (see Bosler paragraph [0073], lines 17-22: time based certificate, time period valid)

e) determining if the one or more configuration directives have been previously received during the time period, by generating a secure hash of the one or more configuration directives and determining if the secure hash is found in memory; (see Bosler paragraph [0078], lines 3-15: hash (i.e. digest) utilized) and

f) only when the date time value is within the time period and the one or more configuration directives have not been previously received during the time period, (see Bosler paragraph [0073], lines 17-22: time-based certificate, time period valid)

performing the steps of:

g) attempting to verify the one or more digital signatures based on generating a secure hash of the one or more configuration directives using the public key and comparing the secure hash to the one or more digital signatures, and applying the configuration directives to a network element only when the one or more

digital signatures are verified successfully. (see Bosler paragraph [0078], lines 3-15: hash generation, authentication)

Regarding Claims 19, 23, 31, Bosler discloses a method as recited in any of Claims 1, 8, or 18, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Regarding Claims 20, 24, 32, Bosler discloses a method as recited in any of Claims 1, 8, or 18, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Regarding Claim 27, Bosler discloses an apparatus as recited in Claim 25, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user,

wherein the second digital signature is applied to a resultant of the first digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Regarding Claim 28, Bosler discloses an apparatus as recited in Claim 25, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Regarding Claim 29, Bosler discloses An apparatus for verifying configuration changes for network devices using digital signatures, comprising: a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a) a processor; (see Bosler paragraph [0067], lines 4-8: processor)
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

b) receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates, received by

user)

c) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

d) attempting to verify the one or more digital signatures based on the trust information; (see Bosler paragraph [0008], lines 7-13: verify digital signature)

e) verifying that two or more digital signatures, from the one or more digital signatures, are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element; (see Bosler paragraph [0008], lines 7-13: verify digital signature)

f) applying the configuration directives to the home network element only when the one or more digital signatures are verified successfully. (see Bosler paragraph [0058], lines 5-14; paragraph [0069], lines 1-5: signature verification, process directive)

Regarding Claims 33, 38, 43, Bosler discloses a computer-readable medium, apparatus as recited in Claims 21, 25, 29, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to perform

the steps of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals (see Bosler paragraph [0058], lines 21-28: receive security information with directive (i.e. command, management message)); applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. (see Bosler paragraph [0058], lines 5-14: digital signature authentication; paragraph [0069], lines 1-5: apply directives or commands after authentication; paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Regarding Claims 34, 39, 44, Bosler discloses a computer-readable medium, apparatus as recited in Claims 21, 25, 29, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13; paragraph [0078], lines 7-15: verification (i.e. validation) with digital signature(s); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Regarding Claims 35, 40, 45, Bosler discloses a computer-readable medium, apparatus as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host network element. (see Bosler paragraph [0073], lines 4-7: security information stored in central location (i.e. host system), (i.e. option, each individual system or host); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Regarding Claims 36, 41, 46, Bosler discloses a computer-readable medium, apparatus as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures. (see Bosler paragraph [0007], lines 6-8: public key cryptography authentication; paragraph [0073], lines 4-7; paragraph [0060], lines 1-6: security information stored in central location or in each individual system or host, certification server (i.e. key server); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Regarding Claims 37, 42, 47, Bosler discloses a computer-readable medium as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures received in a digital certificate and

extracted from the digital certificate as part of attempting to validate the digital signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13: verification (i.e. validation) with digital signature; paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

CVJ
October 1, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/12/07